会員サービス

会員サービス

会員サービスとは、年会費を支払っている会員に対して無償で提供するサービスです。

【　内　容　】

1．経産省推奨の「サイバーセキュリティ経営ガイドライン」の解説を行う
　案① 集合研修型で行う
　案② オンラインセミナーで行う
　案③ オンデマンドで配信する（会員IDにて管理）

2．サイバーセキュリティの概要セミナーを行う
　案① 集合研修型で行う
　案② オンラインセミナーで行う
　案③ オンデマンドで配信する（会員IDにて管理）

3．会員企業のホームページやWebシステムについて、脆弱性診断を行う
　① 基本10ページまでとし、それ以上は有償追加とする
　※．診断（スキャン）のみで、ペネトレーションテスト（攻撃）は行わないこと
　　⇒ いろいろな問題が発生を避けるため、
　　但し、有償追加サービスとしては、個別契約の上あり

サイバーセキュリティ経営ガイドライン

経済産業省が推奨しているガイドラインですが、知識のない人には、わかりづらいので解説が必要。

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

経済産業省
Ministry of Economy, Trade and Industry

文字サイズ変更 小 中 大 アクセシビリティ閲覧支援ツール

サイト内検索 検索 ›拡張検索

ホーム | 経済産業省について | お知らせ | 政策について | 統計 | 申請・お問合せ | English

▸ 政策について ▸ 政策一覧 ▸ 安全・安心 ▸ サイバーセキュリティ政策 ▸ サイバーセキュリティ経営ガイドライン

印刷

サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営ガイドラインの概要

1. 策定の背景

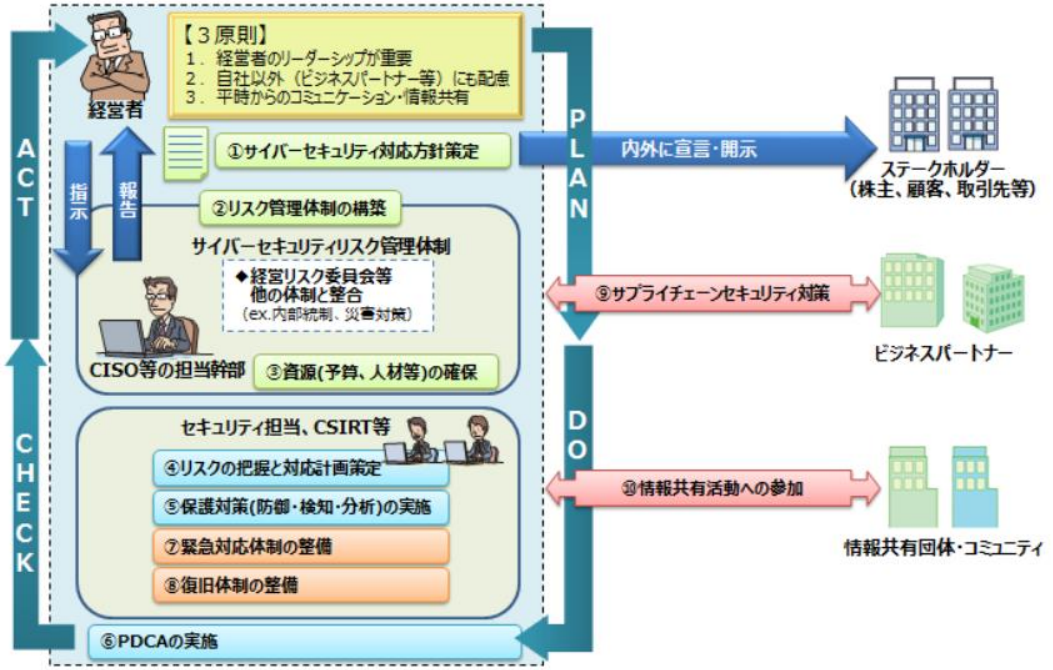
様々なビジネスの現場において、ITの利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化しています。

そこで、企業戦略として、ITに対する投資やセキュリティに対する投資等をどの程度行うかなど、経営者による判断が必要となっています。

2. 概要

経済産業省では、独立行政法人情報処理推進機構（IPA）とともに、大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定しました。

サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者とな



サイバーセキュリティの概要セミナー

サイバーセキュリティの基本的な概要とサイバーインシデントの事例を紹介する。

サイバー攻撃時代への経緯

WannaCryの概要

2017年5月12日正午（英国）から
- 大規模なサイバー攻撃が開始
- 150か国の23万台以上のコンピュータに感染
- 28言語で身代金要求（ビットコイン）

暗号化されコンピュータが使えない

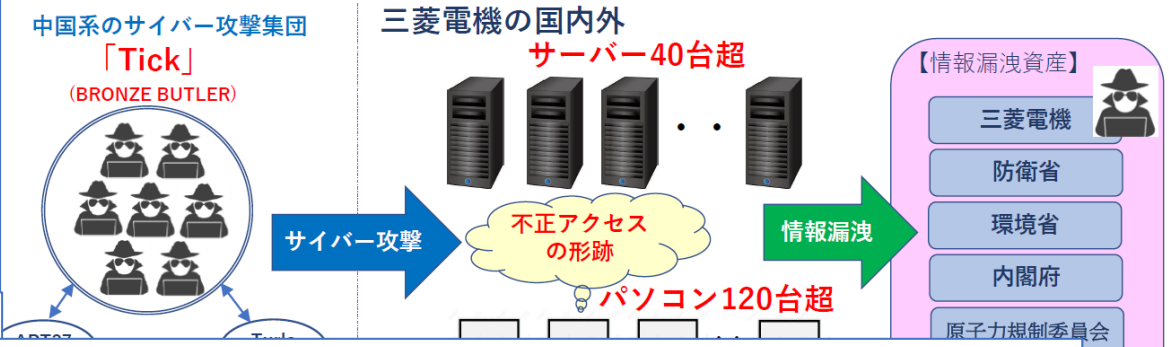
イギリスの国民保険サービスが最初の被害
- 約40の医療施設や7万台の機器が使用不可
- 手術の中止、救急搬送の受入中止など

日本では、12日（金）の夜だった。
IPA（情報処理推進機構）が、土曜、日曜に、この旨を伝え、月曜から怪しげなメールを開かないように、国内にで情報を流した。

WannaCry（ランサムウェア）

身代金を払っても、暗号化は解除されなかった

三菱電機、サイバー攻撃 （2020年1月20日ニュース）



NEC、サイバー攻撃 （2020年1月30日ニュース）

防衛省関連の約2万8000件のファイルに不正アクセスがあった。

2016年12月	サイバー攻撃開始	未知のマルウェアに感染したが、検知できなかった。
2017年6月	社内PC不正通信⇒隔離	社内PCの不正通信が見つかりネットワークから離脱した。
2018年7月	不正アクセス確認	防衛事業部にて約2万7455件のファイルに不正アクセスがあった。 ⇒ 防衛省には説明済という
2020年1月30日	サイバー攻撃を公表	

1年8か月

脆弱性診断

会員には、オープンソースのツールを使って、脆弱性診断を行い、評価レポートと解説（報告会）を行う

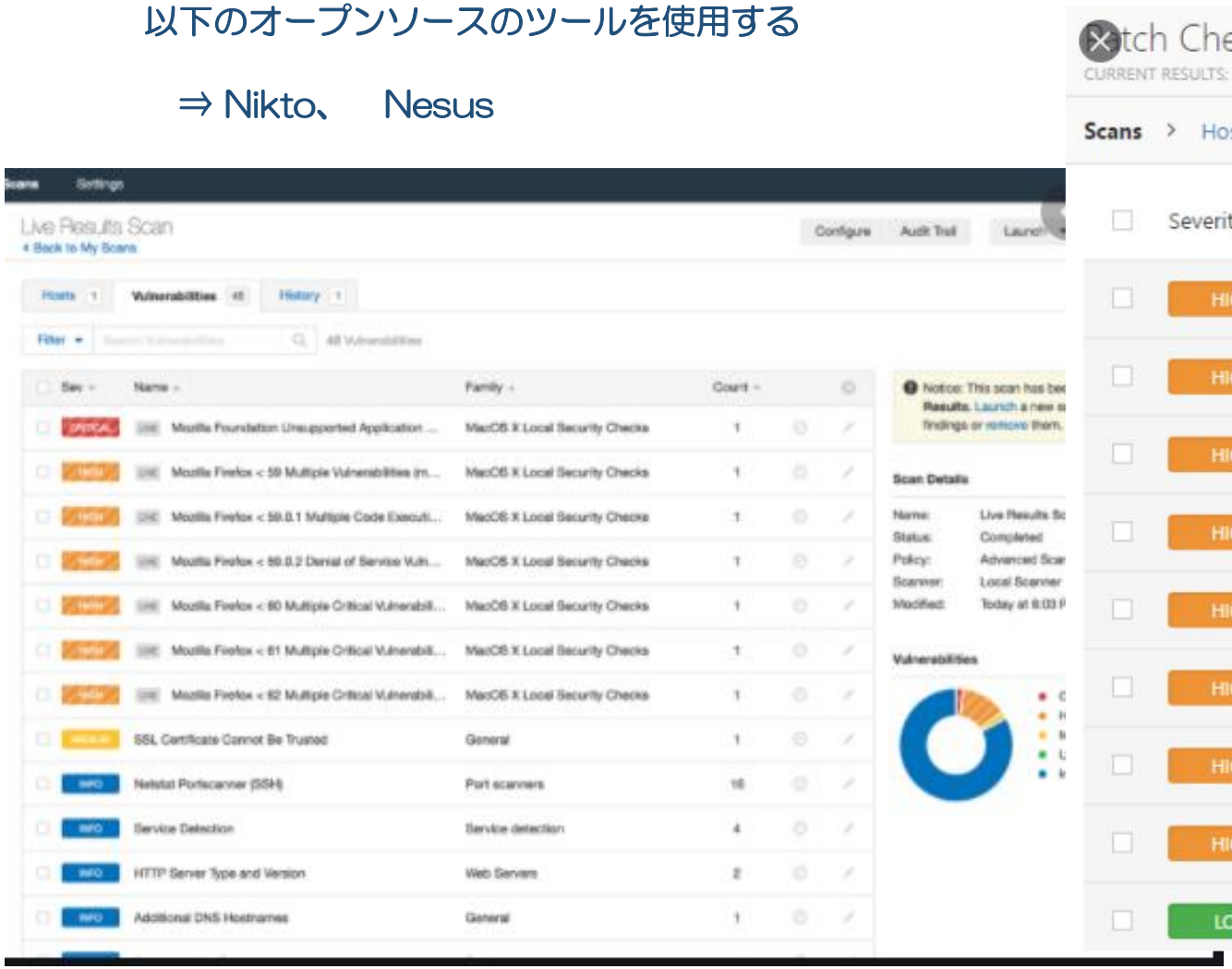
OWASP Top10に準拠して、Webアプリケーションの脆弱性診断を行う。

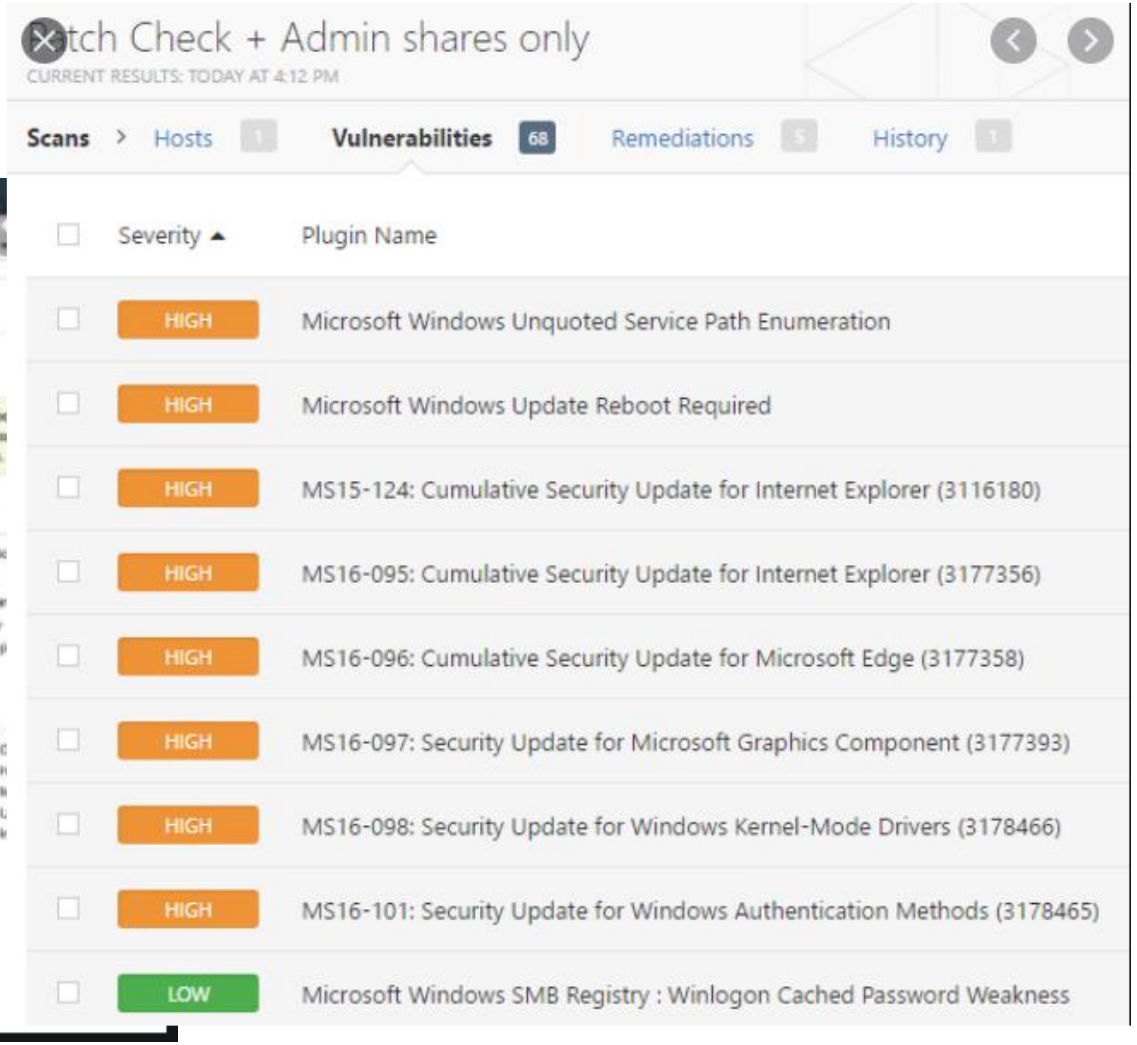
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – インジェクション	→	A1:2017-インジェクション
A2 – 認証の不備とセッション管理	→	A2:2017-認証の不備
A3 – クロスサイトスクリプティング (XSS)	↘	A3:2017-機微な情報の露出
A4 – 安全でないオブジェクトへの直接参照 [A7とマージ]	U	A4:2017-XML 外部エンティティ参照 (XXE)[NEW]
A5 – 不適切なセキュリティ設定	↘	A5:2017-アクセス制御の不備 [マージ]
A6 – 機微な情報の露出	↗	A6:2017-不適切なセキュリティ設定
A7 – 機能レベルのアクセス制御の不足 [A4とマージ]	U	A7:2017-クロスサイトスクリプティング (XSS)
A8 – クロスサイトリクエストフォージェリ (CSRF)	☒	A8:2017-安全でないデシリアライゼーション [NEW,コミュニティ]
A9 – 既知の脆弱性のあるコンポーネントの使用	→	A9:2017-既知の脆弱性のあるコンポーネントの使用
A10 – 未検証のリダイレクトと転送	☒	A10:2017-不十分なロギングとモニタリング[NEW,コミュニティ]

脆弱性診断ツール

以下のオープンソースのツールを使用する

⇒ Nikto、　Nesus





追加有償オプション

追加オプションとして、サービスを提供する

1．サキュリティコンサル

2．ペネトレーションテスト

3．追加脆弱性診断

4．サイバーセキュリティトレーニング